PERFORMANCE WORK STATEMENT

Contract: **N66001-15-D-0056**
Task Order: **0004**
Tracking Number: **5201-H0008**
Task Title: Pacific Fleet AOR SCI Networks Support
Date: 22 September 2015

1.0 SCOPE

1.1 This is a Level of Effort (LOE) service acquisition to provide engineering and information assurance support work to be undertaken to accredit, test, and modernize the Multinational Intelligence Interoperability Initiative (MI3) systems on Pacific Fleet force level ships (see table 1) and at the Third Fleet Maritime Headquarters Maritime Operations Centers (MOC) ashore for Space and Naval Warfare (SPAWAR) Systems Center Pacific, Pacific C4ISR Department, Code H, Pearl City, Hawaii. The project scope includes three distinct Sensitive Compartmented Information (SCI) networks on (b)(3) force level ships home ported in Pacific Fleet (PACFLT) Area of Responsibility (AOR) and three shore-based Maritime Headquarters with Maritime Operational Center (MOC). See table 1 for initial listing. Additional ship and shore locations may be rolled over and/or added to option years.

Table 1: MI3 Locations

Hull	Ship	Homeport	Hopper Regional Maintenance Division
(b)(3)			ISC-OFE
			ISC-OFE
			ISC-OFE
			ISC-ONW
			ISC-ONW
			ISC-OSW
			ISC-OSW
			ISC-OSW
			ISC-OSW
			ISC-OSW
			ISC-OSW
			ISC-OHI
			ISC-OFE

2.0 APPLICABLE DOCUMENTS

2.1 OPNAVINST F3300.53C (Series), Navy Antiterrorism Program

2.2 DOD 5220.22-M (Series), National Industrial Security Program Operating Manual (NISPOM)

2.3 National Security Decision Directive 298 (Series), National Operations Security Program (NSDD) 298

2.4 DOD 5205.02E (Series), DOD Operations Security (OPSEC) Program

2.5 OPNAVINST 3432.1A (Series), DON Operations Security

2.6 SPAWARINST 3432.1 (Series), Operations Security Policy

2.7 DOD Instruction 8510.01 March 23, 2014 Risk Management Framework (RMF) For DOD Information Technology (IT)

2.8 Intelligence Community Directive #503 (ICD 503)

2.9 Navy SCI Information Assurance Program Risk Management Framework Implementation Plan (Appendix G)

3.0 TECHNICAL REQUIREMENTS

3.1 Restore Multinational Intelligence Interoperability Initiative (MI3) capability to as many specific sites as resources, timeline, and platform availabilities permit, to include a minimum of one of each afloat platform type (b)(6)

3.2 Coordinate with Space and Naval Warfare Systems Command (SPAWARSYSCOM) and Consolidated Afloat Networks and Enterprise Services (CANES) Program Management Office (PMO) for integration testing and approval.

3.3 Coordinate with platform Type Commanders (TYCOMs) ((Naval Air Systems Command (NAVAIR) and Naval Sea Systems Command (NAVSEA)) to ensure compliance with shipboard systems installation process and Ship Change Documents (SCD).

3.4 Coordinate with Defense Intelligence Agency (DIA) Pacific to leverage available Information Technology (IT) services and Information Assurance (IA) security controls on MI3 networks.

3.5 Coordinate with West Continental United States (CONUS) Regional Information System Security Manager (ISSM) to ensure compliance with Intelligence Community Directive (ICD)-503 authorization and accreditation Risk Management Framework (RMF) (referenced in paragraph 2.7) process as implemented by Navy SCI Chief Information Security Officer (CISO).

3.6 Develop or collect necessary documentation for each Risk Management Framework (RMF) step.

3.7 Post and maintain all documentation in a common Joint Worldwide Intelligence Communications System (JWICS) location identified by Hopper Information Service Center (ISC).

3.8 Collect and aggregate current footprint and documentation and verify current operational status for existing MI3 locations via on-line coordination with users and Hopper ISC.

3.9 Obtain schedule information from SPAWARSYSCOM Code PMW-160 planned CANES migration for all sites.

3.10 Conduct functional requirement analysis to verify continued requirement for existing capability and elicit any new functional requirements from customer commands.

3.11 Provide information to Hopper ISC to assist in developing Information Assurance brief categorizing MI3 information system (RMF Step 1) (referenced in paragraph 2.7).

3.12 Perform analysis of alternatives (AOA) for (a) restoring and refreshing existing three-network solution with modern hardware and software and reutilizing existing encryption devices and (b) out-sourcing multi-domain solution to DIA (e.g. Next Generation Desktop Environment (NGDE) that would allow login to each releasable domain from single desktop hardware and single network connection (JWICS). Anticipate that in the interest of rapid restoration of capability to Forward Deployed Naval Forces (FDNF) and near-term deploying platforms, two increments of design solutions may be required: (1) Increment One relying on modernization of existing three-domain solution for installations targeted prior to Fiscal Year 16-Quarter3 and (2) Increment Two leveraging DIA services and design to deliver a single platform, multi-domain solution for installations targeted in Fiscal Year 16-Quarter 3 and beyond.

3.13 Develop preliminary design solutions for both alternatives and present Design Options Brief.

3.14 Subsequent to Hopper ISC decision on Design Options Brief, develop and provide a detailed design and project schedule to include a bill of materials (BOM) and estimated staffing level of effort to implement the solution.

3.15 Generate templates, instructions, and training guides for site survey, installation, and system operations verification test (SOVT) that can be executed by Hopper ISC

government personnel (primarily Sailors) from the IT Operations Division based in same region as the target ship or MOC.

3.16 Coordinate site installation sequence per COMMANDER, U.S PACIFIC FLEET N2 priorities and individual ship deployment schedules.

3.17 Provide MI3 training (via video teleconference (VTC)) to Hopper ISC personnel based in PACFLT AOR.

3.18 In coordination with Hopper ISC personnel, support assessment readiness review and assessment of security controls (RMF Step 4) (referenced in paragraph 2.7).

3.19 Observe and support additional installation planning necessary to complete prerequisite tasks.

3.20 Obtain designation as a MI3 Trusted Agent (TA) in accordance with paragraph 2.8 and 2.9. This will require on the job training by Department of the Navy (DON) government personnel, existing Security Control Assessors (SCAs) or existing SCA TAs for same system.

3.21 Provide remote technical advice for all subsequent installations.

3.22 Provide technical assistance to MI3 sites for casualty restoral for first ninety days after installation. Coordinate transition of subsequent and continuing technical assistance to the appropriate Hopper ISC IT Operations Regional Maintenance Cell.

3.23 Make recommendations to Hopper ISC for efficient and effective monitoring of deployed MI3 systems (RMF Step 6).

3.24 Provide wide area network (WAN) and local area network (LAN) communications engineering expertise for the WAN and LAN operating nodes of the JWICS network throughout the Southwestern CONUS Region.

3.25 Perform network operational evaluations, maintain configuration management for the networks, and perform administrative and corrective actions for the JWICS and coalition networks employing cryptographic system protection.

3.26 Perform the testing, evaluation and system implementation of new, approved Government Furnished Material (GFM) IA products within existing connectivity infrastructure.

3.27 Provide network security performance, network operational performance evaluations and data reports for JWICS shore-based nodes. Use Solar Winds network monitory software (provided by the government) as the primary tool for real-time monitoring and daily/weekly automated reports. Also, provide monthly narrative of any network security

vulnerabilities or performance trends or potential issues that meet criteria for alerting government to take action **(CDRL A001)**.

3.28 Produce installation design and as-built documents **(CDRL A008)**.

3.29 Observe and validate the testing of new installations performed/completed by third-parties.

3.30 Assist in registering and bringing new JWICS sites into the operational network.

3.31 In coordination with on-site personnel, remotely troubleshoot, identify and recommend corrections to potential and emergent network and system operational and information security problems at all layers of the system including: JWICS-wide, WAN, and LAN.

3.32 Follow DIA JWICS reporting procedures and report all classified actions internally using Siebel incident/even management and workflow software (provided by the government) (via web interface), supplemented by phone and email.

3.33 The contractor shall complete a Contractor's Progress, Status and Management Report monthly **(CDRL A001)**. Included will be a network security report, specified in paragraph 3.27.

3.34 The contractor shall complete a Contractor Roster Report monthly **(CDRL A002)**. The report shall list all contractor personnel assigned to execute tasking.

4.0 GOVERNMENT FURNISHED INFORMATION/MATERIAL/PROPERTY

None.

5.0 CONTRACTOR FURNISHED MATERIAL

None.

6.0 TRAVEL

6.1 The following travel is for estimating purposes only. It is anticipated that the following travel requirements may be necessary for the Base Year and Option Years 1 through 4 (same locations for both base year and all option years):

6.1.1 San Diego, CA to (b)(3) – one (1) person, five (5) trips for seven (7) days each.

6.1.2 San Diego, CA to (b)(3) – one (1) person, two (2) trips for seven (7) days each.

6.1.3 San Diego, CA to (b)(3) – one (1) person, two (2) trips for seven (7) days each.

6.1.4 San Diego, CA to (b)(3) – one (1) person, one (1) trip for seven (7) days.

Note: All travel and/or travel changes shall be requested in writing and approved in advance by the Contracting Officer's Representative.

7.0 SECURITY

7.1 The work to be performed under this task shall be at the Top Secret (TS)/Sensitive Compartmented Information (SCI) level.

7.2 Key personnel assigned to this effort who require access to SCI data and spaces must possess a current single scope background (SSBI) with ICD 704 eligibility (which replaced DCID 6/4 eligibility).

7.3 The candidate must have previously passed a [counter-intelligence (CI) or full-scope (FS)] polygraph test or schedule to take and pass a polygraph test upon request by the Government in order to gain access into the work space described in paragraph 1.1 of this PWS. Failure to possess or pass a polygraph test is reason to deny personnel suitability for this task.

7.4 Anti-Terrorism/Force Protection (AT/FP) briefings are required for all personnel (Military, DOD Civilian, and contractor) per OPNAVINST F3300.53C. Contractor employees must receive the AT/FP briefing annually. The briefing is available at https://atlevel1.dtic.mil/at/, if experiencing problems accessing this website contact ssc_fortrav@navy.mil.

7.5 As required by National Industrial Security Program Operating Manual (NISPOM) Chapter 1, Section 3, contractors are required to report certain events that have an impact on: 1) the status of the facility clearance (FCL); 2) the status of an employee's personnel clearance (PCL); 3) the proper safeguarding of classified information; 4) or an indication that classified information has been lost or compromised. Contractors working under SSC Pacific contracts will ensure information pertaining to assigned contractor personnel are reported to the Contracting Officer Representative (COR)/Technical Point of Contact (TPOC), the Contracting Specialist, and the Security's COR in addition to notifying appropriate agencies such as Cognizant Security Agency (CSA), Cognizant Security Office (CSO), or Department Of Defense Central Adjudication Facility (DODCAF) when that information relates to the denial, suspension, or revocation of a security clearance of any assigned personnel; any adverse information on an assigned employee's continued suitability for continued access to classified access; any instance of loss or compromise, or suspected loss or compromise, of classified information; actual, probable or possible espionage, sabotage, or subversive information; or any other circumstances of a security nature that would affect the contractor's operation while working under SSC Pacific contracts.

7.6 **Operations Security:** OPSEC is a five step analytical process (identify critical information; analyze the threat; analyze vulnerabilities; assess risk; develop

countermeasures) that is used as a means to identify, control, and protect unclassified and unclassified sensitive information associated with U.S. national security related programs and activities. All personnel working under this task will at some time handle, produce or process Critical Information or CPI, and therefore all Contractor personnel must practice OPSEC. All work is to be performed in accordance with DoD OPSEC requirements, and in accordance with the OPSEC attachment to the DD254.

8.0 **Information Assurance(IA)/Cybersecurity:**

The following workforce categories, levels, training, and certifications are required for contractor personnel under this task order: Information Assurance Technical (IAT) Level I is required, with Security+ serving as primary qualifying certification.

The Contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions Ser 83010/ 11-01 83010 SSC Pacific- Information Assurance January 11, 2011 identified in section 8.0 of this PWS in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet applicable information assurance certification requirements, including (a) DoD-approved IA workforce certifications appropriate for each specified category and level and (b) appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions. The contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions, reporting current IA certification status and compliance using CDRL Contractor Roster, DI-MGMT-81596 in the format prescribed by the COR.

9.0 PLACE OF PERFORMANCE

9.1 Hopper IT Operations Southwest Division (ISC-OSW), at Center for Information Dominance Unit (CIDU) San Diego, CA and at deployed locations throughout the theater.

10.0 PERFORMANCE BASED CRITERIA

10.1 Performance Requirement

The contractor shall provide services and deliverables in accordance with this Performance Work Statement (PWS) and in accordance with the attached task order CDRL Form 1423-1.

10.2 Performance Standard

The contractor's performance shall meet all of the requirements of this PWS and comply with all applicable guidance, directives, and standards. The contractor shall deliver all task order data items in accordance with the authorities, content, format, media, marking,

applications, quantities, frequency and submission date, delivery method, addressee, and Department of Defense form 250 requirements specified in the CDRL for each data item.

10.3 Acceptable Quality Level

The effectiveness of the contractor's services and/or deliverables will be measured for 100% compliance with the PWS and CDRL requirements.

10.4 Method of Surveillance

The Government will monitor and assess the contractor's performance against the Acceptable Quality Level in accordance with this task order's Quality Assurance Surveillance Plan (QASP).

10.5 Incentive

Failure to meet acceptable quality levels may result in an unsatisfactory past performance report by the Government.